

AMENDMENTS TO THE CLAIMS

Claims pending

- At time of the Action: Claims 1-54.
- After this Response: Claims 1-54.

Canceled or Withdrawn claims: None

Amended claims: None

New claims: None

1. **(Original)** A method comprising:
deriving a secret that is unique to a game console running a particular game
title; and
establishing a secure communication link between multiple game consoles
over a local area network using the secret.

2. **(Original)** A method as recited in claim 1, wherein the deriving
comprises deriving the secret from data stored in the game console and data
associated with the particular game title.

3. **(Original)** A method as recited in claim 1, wherein the deriving
comprises:
retrieving a console-based key from the game console and a title-based key
associated with the particular game title; and
deriving the secret from the console-based key and the title-based key.

1 4. **(Original)** A method as recited in claim 1, wherein the establishing
2 comprises:

3 discovering whether another game console on the local area network is
4 hosting the particular game title; and

5 exchanging secure communication keys between the multiple game
6 consoles to facilitate secure multi-console play of the particular game title over the
7 local area network.

8
9 5. **(Original)** A method as recited in claim 1, wherein the establishing
10 comprises establishing a secure communication link over an Ethernet segment
11 using the secret.

12
13 6. **(Original)** A method comprising:

14 generating at least one key that is secret to an authentic gaming system
15 running an authentic game title;

16 discovering whether another gaming system on a common local area
17 network is hosting the game title; and

18 establishing a secure communication link between multiple gaming systems
19 to facilitate multi-system play of the game title over the local area network.

20
21 7. **(Original)** A method as recited in claim 6, wherein the generating
22 comprises:

23 retrieving a console-based key from the gaming system and a title-based
24 key associated with the game title; and

25 deriving the key from the console-based key and the title-based key.

1 8. **(Original)** A method as recited in claim 6, wherein the discovering
2 comprises broadcasting, over the local area network, a request to join in playing
3 the game title being hosted by another gaming system.

4
5 9. **(Original)** A method as recited in claim 8, wherein the discovering
6 comprises receiving a broadcast reply, over the local area network, from the
7 gaming system that is hosting the game title.

8
9 10. **(Original)** A method as recited in claim 6, wherein the discovering
10 comprises:

11 cryptographically encoding, using a generated key, a request to join in
12 playing the game title being hosted by another gaming system; and
13 broadcasting the request over the local area network.

14
15 11. **(Original)** A method as recited in claim 6, wherein the discovering
16 comprises broadcasting a request over an Ethernet segment.

17
18 12. **(Original)** A method as recited in claim 6, wherein the establishing
19 comprises exchanging secure communication keys between the multiple game
20 consoles to facilitate multi-console play of the particular game title over the local
21 area network.

22
23 13. **(Original)** In a networked gaming environment where multiple
24 game consoles are connected via a local area network, a method comprising:
25

1 broadcasting, from a client game console over a local area network, a
2 request to join in playing a game title in a network gaming session being hosted by
3 a host game console, the request containing a secret that is unique to the client
4 game console running the game title; and

5 broadcasting, from the host game console over the local area network, a
6 reply to the request, the reply containing information that can be used to establish
7 a secure communication link.

8
9 14. (Original) A method as recited in claim 13, further comprising
10 deriving the secret from data stored in the client game console and data associated
11 with the game title.

12
13 15. (Original) A method as recited in claim 13, wherein the local area
14 network comprises an Ethernet segment.

15
16 16. (Original) A method comprising:
17 retrieving a console-based key stored on a game console;
18 retrieving a title-based key associated with a game title running on the
19 game console; and
20 deriving one or more keys from the console-based key and the title-based
21 key.

22
23 17. (Original) A method as recited in claim 16, wherein the deriving
24 comprises computing a hashing function on a concatenation of the console-based
25 key and the title-based key.

1 18. **(Original)** One or more computer-readable media comprising
2 computer-executable instructions that, when executed, perform the method as
3 recited in claim 16.
4

5 19. **(Original)** In a networked gaming environment where multiple
6 game consoles are connected via a local area network, a method comprising:

7 creating a request to join in playing a game title being hosted by a host
8 game console on the local area network;

9 broadcasting the request over the local area network;

10 receiving a reply from the host game console, the reply containing one or
11 more session keys; and

12 using the session keys from the reply to facilitate future secure
13 communication with the host game console.
14

15 20. **(Original)** A method as recited in claim 19, wherein the
16 broadcasting comprises broadcasting the request over an Ethernet segment.
17

18 21. **(Original)** A method as recited in claim 19, further comprising
19 cryptographically encoding the request prior to the broadcasting.
20

21 22. **(Original)** A method as recited in claim 19, wherein the receiving
22 comprises listening for a reply that is broadcast from the host game console over
23 the local area network.
24
25

1 23. **(Original)** A method as recited in claim 22, wherein the broadcast
2 reply is cryptographically encoded, and further comprising cryptographically
3 decoding the reply.

4
5 24. **(Original)** One or more computer-readable media comprising
6 computer-executable instructions that, when executed, perform the method as
7 recited in claim 19.

8
9 25. **(Original)** In a networked gaming environment where multiple
10 game consoles are connected via a local area network and at least two game
11 consoles are playing a same game title, a method comprising:

12 forming an initial packet that contains first data used to derive a
13 cryptographic key;

14 computing a first hash digest of the initial packet;

15 sending the initial packet and the first hash digest to another game console
16 on the local area network that is playing the same game title;

17 receiving a reply packet from the other game console, the reply packet
18 including a second hash digest and second data;

19 authenticating the reply packet using the second hash digest; and

20 deriving one or more security association keys from the first and second
21 data, the security association keys being used to secure communication between
22 the multiple consoles.

1 26. **(Original)** One or more computer-readable media comprising
2 computer-executable instructions that, when executed, perform the method as
3 recited in claim 25.

4
5 27. **(Original)** In a networked gaming environment where multiple
6 game consoles are connected via a local area network, a method comprising:

7 retrieving a console-based key from a first game console and a title-based
8 key associated with a game title running on the first game console;

9 deriving at least one cryptographic key from the console-based key and the
10 title-based key;

11 creating, at a first console, a request to join in playing the game title being
12 hosted by a second game console on the local area network;

13 cryptographically encoding the request using the cryptographic key;

14 broadcasting the request over the local area network;

15 cryptographically decoding the request, at the second game console, using
16 the cryptographic key;

17 generating, at the second game console, a reply that contains at least one
18 session key;

19 cryptographically encoding the reply using the cryptographic key;

20 broadcasting the reply over the local area network;

21 cryptographically decoding the reply, at the first game console, using the
22 cryptographic key;

23 exchanging packets between the first and second game consoles, the
24 packets being protected using the session key and containing data used to derive at
25 least one security association key; and

1 establishing a secure communication link between the first and second
2 game consoles using the security association keys to facilitate secure multi-
3 console play of the game title.
4

5 28. **(Original)** A method as recited in claim 27, wherein the deriving
6 comprises computing a hashing function on a concatenation of the console-based
7 key and the title-based key.
8

9 29. **(Original)** A method as recited in claim 27, wherein:
10 the deriving comprises computing an encryption key and a signature key;
11 and

12 the encoding of the request comprises encrypting the request using the
13 encryption key to form an encrypted request and digitally signing the encrypted
14 request using the signature key.
15

16 30. **(Original)** A method as recited in claim 27, wherein the exchanging
17 comprises:

18 forming, at one of the first or second game consoles, a packet that contains
19 the data used to derive the security association key;

20 computing a hash digest of the packet;

21 sending the packet and the hash digest to the other of the first or second
22 game consoles; and

23 authenticating the packet using the hash digest at the other first or second
24 game consoles.
25

1 31. **(Original)** A method as recited in claim 27, wherein the data used
2 to derive the security association key comprises values used by a cryptographic
3 Diffie-Hellman function.

4
5 32. **(Original)** One or more computer-readable media comprising
6 computer-executable instructions that, when executed, perform the method as
7 recited in claim 27.

8
9 33. **(Original)** In a networked gaming environment where multiple
10 game consoles are connected via a local area network, a method comprising:

11 retrieving a console-based key from a first game console and a title-based
12 key associated with a game title running on the first game console;

13 deriving at least one cryptographic key from the console-based key and the
14 title-based key;

15 creating a request to join in playing the game title being hosted by another
16 game console on the local area network;

17 encoding the request using the cryptographic key;

18 broadcasting the request over the local area network;

19 receiving a reply from a host game console, the reply containing at least
20 one session key;

21 exchanging packets with the host game console, the packets being protected
22 using the session key and containing data used to derive at least one security
23 association key; and

24 establishing a secure communication link with the host game console using
25 the security association key.

1 34. **(Original)** A method as recited in claim 33, wherein the receiving
2 comprises listening for a reply that is broadcast from the host game console over
3 the local area network.

4
5 35. **(Original)** One or more computer-readable media comprising
6 computer-executable instructions that, when executed, perform the method as
7 recited in claim 33.

8
9 36. **(Original)** In a networked gaming environment where multiple
10 game consoles are connected via a local area network, a method comprising:

11 retrieving a console-based key from a first game console and a title-based
12 key associated with a game title running on the first game console;

13 deriving at least one cryptographic key from the console-based key and the
14 title-based key;

15 receiving a request to join in playing the game title from another game
16 console on the local area network;

17 cryptographically decoding the request using the cryptographic key;

18 generating a reply that contains at least one session key;

19 encoding the reply using the cryptographic key;

20 sending the reply over the local area network;

21 exchanging packets with the other game console, the packets being
22 protected using the session key and containing data used to derive at least one
23 security association key; and

24 establishing a secure communication link with the other game console
25 using the security association key.

1 37. **(Original)** A method as recited in claim 33, wherein the sending
2 comprises broadcasting the reply over the local area network.

3
4 38. **(Original)** One or more computer-readable media comprising
5 computer-executable instructions that, when executed, perform the method as
6 recited in claim 33.

7
8 39. **(Original)** A computer-readable medium for a game console
9 comprising computer-executable instructions that, when executed, direct the game
10 console to:

11 obtain a first key stored in memory of the game console and a second key
12 associated with a game title running on the game console; and

13 derive one or more keys from the first and second keys.

14
15 40. **(Original)** A computer-readable medium for a game console
16 comprising computer-executable instructions that, when executed, direct the game
17 console to:

18 encrypt a request to join in playing a game title being hosted by a remote
19 host game console on a local area network;

20 digitally sign the request;

21 broadcast the request over the local area network;

22 listen for at least one broadcast reply from the host game console;

23 upon receipt of the reply, extract at least one session key from the reply for
24 use in facilitating future communication with the host game console;

1 form an initial packet that contains first data used to derive a cryptographic
2 key;
3 compute a first hash digest of the initial packet using the session key;
4 send the initial packet and the first hash digest to the host game console;
5 listen for a reply packet from the host game console, the reply packet
6 including a second hash digest and second data;
7 authenticate the reply packet using the session key and the second hash
8 digest; and
9 derive at least one security association key from the first and second data,
10 the security association keys being used to secure communication with the host
11 game console.

12
13 41. (Original) A computer-readable medium for a game console
14 comprising computer-executable instructions that, when executed, direct the game
15 console to:

16 receive a request from a remote game console on a local area network, the
17 request seeking network play of a game title;

18 authenticate the request as being generated by an authentic game console
19 running an authentic version of the game title;

20 decode the request;

21 determine whether to allow the remote game console to play;

22 in an event the remote game console is allowed to play, create a reply with
23 containing at least one session key;

24 encrypt and digitally sign the reply;

25 send the reply to the remote game console;

1 receive an initial packet directly from the remote game console, the initial
2 packet containing first data used to derive a cryptographic key;
3 authenticate the initial packet using the session key;
4 form a response packet holding second data used to derive a cryptographic
5 key;
6 send the response packet to the remote game console; and
7 derive at least one security association key from the first and second data,
8 the security association keys being used to secure communication with the remote
9 game console.

10
11 42. (Original) A computer-readable medium as recited in claim 41,
12 further comprising computer-executable instructions that, when executed, direct
13 the game console to broadcast the response packet over the local area network.

14
15 43. (Original) A game console, comprising:
16 a memory to store a first key;
17 a game title configured to execute on the game console, the game title
18 having an associated second key; and
19 a processor coupled to the memory, the processor being configured to
20 derive at least one cryptographic keys from the first and second keys.

21
22 44. (Original) A game console as recited in claim 43, wherein the
23 memory comprises a read only memory.
24
25

1 45. **(Original)** A game console as recited in claim 43, wherein the
2 processor is configured to compute a hash function of the first and second keys.

3
4 46. **(Original)** A game console as recited in claim 43, wherein the
5 processor is further configured to discover another game console on a local area
6 network that is hosting the game title.

7
8 47. **(Original)** A game console as recited in claim 43, wherein the
9 processor is further configured to use the cryptographic key to establish a secure
10 communication link with a remote game console over a local area network.

11
12 48. **(Original)** A game console, comprising:
13 a memory; and
14 a processor coupled to the memory and configured to generate at least one
15 key that is secret to the game console when running an authentic game title, the
16 processor being further configured to discover, using the key, a host game console
17 on a common local area network that is hosting the game title and to establish a
18 secure communication link with the host game console over the local area
19 network.

20
21 49. **(Original)** A game console as recited in claim 48, wherein the
22 processor is configured to derive the key from data stored in the memory and data
23 associated with the authentic game title.
24
25

1 50. **(Original)** A game console as recited in claim 48, wherein the
2 processor is further configured to discover a host game console by creating a
3 request to join in playing the game title and broadcasting the request over the local
4 area network.

5
6 51. **(Original)** A game console as recited in claim 48, wherein the
7 processor establishes the secure communication link by exchanging data with the
8 host game console that can be used to derive a cryptographic key.

9
10 52. **(Original)** A system, comprising:
11 first and second game consoles with network connections to facilitate
12 connection to a local area network, the first and second game consoles running a
13 same game title and being configured to generate identical keys by virtue of
14 running the same game title; and
15 the first game console being configured to discover the second game
16 console by broadcasting messages over the local area network, the messages being
17 secured by the keys.

18
19 53. **(Original)** A system as recited in claim 52, where in the first and
20 second game consoles are configured to establish a secure communication link
21 over the local area network by exchanging data used to derive a cryptographic key.

22
23 54. **(Original)** A system as recited in claim 52, where in the local area
24 network comprises an Ethernet segment.
25